THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

KATHY NEAL individually and on behalf of all others similarly situated, Plaintiff, v. DELOITTE CONSULTING LLP, Defendant.	**Case No.** 1:20-cv-04362 **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

I. INTRODUCTION

1. Businesses that collect and store sensitive information about their customers have a duty to safeguard that information and ensure it remains private. This responsibility is essential where a business keeps and stores its customers' highly personal information, such as their names, email addresses, phone numbers, social security numbers, and/or bank account and/or routing information.

2. Plaintiff Kathy Neal brings this class action individually and on behalf of individuals that suffered, and continue to suffer, damages as a result of Defendant Deloitte Consulting LLP's ("Deloitte" or the "Defendant") failure to properly secure and safeguard the Personally Identifying Information described above ("PII" or "PII").

3. Specifically, as part of the federal government's Pandemic Unemployment Assistance ("PUA") program, Deloitte formed contracts with various state agencies – including the Ohio Department of Job and Family Services ("ODJFS"), the Illinois Department of Employment Security ("IDES"), the Colorado Department of Labor and Employment ("CDLE") and the Arkansas Division of Workforce Services ("ADWS") – to help those states administer the PUA program by designing, building, and maintaining web-based portals through which individuals may apply for unemployment benefits and communicate with state officials.

4. In May 2020, officials from these state agencies publicly announced that these digital systems Deloitte designed, built and maintained allowed public access to unemployment applicants' PII, including but not limited to their name, social security number, and street address associated with your PUA claim, exposing this sensitive private data to unauthorized third parties (the "Data Breach").

5. On May 21, 2020, Plaintiff received correspondence from Deloitte confirming this breach and informing Plaintiff of the following:

> A limited data access issue recently occurred within the new Pandemic Unemployment Assistance (PUA) system. An analysis found that one PUA claimant was able to inadvertently access personal information of a limited number of other PUA claimants when logged into the system last week. That same claimant reported the issue and within an hour, it was corrected to prevent any future unauthorized access.
>
> The information viewed by this one person may have included your name, social security number, and street address associated with your PUA claim. Immediately upon learning of this issue, Deloitte Consulting LLP (Deloitte), the vendor who built and maintains the PUA portal for IDES, began an investigation and stopped any further unauthorized access of claimants' personal information.
>
> Based upon that investigation, there is no indication that your personal information was improperly used or is likely to be misused.
>
> Out of an abundance of caution, Deloitte is offering you the option of enrolling in 12 months of free credit monitoring. A one-year membership of Experian's® IdentityWorks℠ identity protection service is available to you, at no cost. Attached to this email is a flyer from Experian IdentityWorks℠ describing the service and providing detailed instructions.
>
> To enroll online for the Experian IdentityWorks℠ credit monitoring service, you can go to the Experian site using the link below. You will be instructed how to initiate the online membership and will need to provide your personal information requested for enrollment. You will also be asked to provide the code listed below to reflect the pre-paid purchase of the credit monitoring service. If you prefer, you can enroll on the phone by speaking with the Experian Customer Care team at 877.890.9332. Please provide engagement number DB20234 as proof of eligibility for the Experian credit monitoring services.
>
> You will have until August 30, 2020, to activate this membership, which will then continue for 12 full months from the date of activation.
>
> Code and link:
>
> •Pre-paid Code: […]
> •Link: […]
>
> In addition, federal law entitles everyone to one free credit report per year from each of the three main credit bureaus, and you can obtain information regarding fraud alerts and security freezes from them:

Equifax (800) 525-6285
P.O. Box 740241
Atlanta, GA 30374
www.equifax.com <http://www.equifax.com/

TransUnion (800) 680-7289
P.O. Box 2000
Chester, PA 19022
www.tuc.com

Finally, to find out more about protecting personal information, visit the Illinois Attorney General's webpage at www.illinoisattorneygeneral.gov and/or the Federal Trade Commission:

Federal Trade Commission, (202) 326-2222
Bureau of Consumer Protection
Federal Trade Commission
600 Pennsylvania Ave, NW
Washington, DC 20580
https://www.ftc.gov

We apologize for any concerns or inconvenience that this incident has caused. Please be assured that we take very seriously our responsibility to safeguard the personal information you entrust to our care, and deeply regret that this incident occurred.

6. As a result of Deloitte's failure to properly safeguard their sensitive PII, Plaintiff and the Members of the Class(es) asserted herein.

II. PARTIES

7. Plaintiff Kathy Neal resides in and is a citizen of Illinois.

8. Plaintiff applied for unemployment benefits through the web-portal created and maintained by Deloitte, and Plaintiff's PII was left publicly accessible. As a result of the Plaintiff's data being exposed, credit inquiries were made in Plaintiff Neal's name to open accounts that she did not authorize. By way of example, Plaintiff received notice of credit inquiries in Plaintiff Neal's name without her consent with Westlake Financial Services and with FingerHut. As a result of this fraudulent activity, Plaintiff Neal's credit score dropped drastically.

9. Credit Score points are valuable. As you add points to your score, you'll have access to more credit products — and pay less to use them. "Depending on your credit history, a 15- or 20-point shift could mean the difference between being approved or declined or better terms or higher costs," said Rod Griffin, the director of public education at Experian, a major credit-reporting firm.[1]

10. As a result of Deloitte's failure to adequately safeguard Plaintiff's PII, Plaintiff was injured. Additionally, Plaintiff has been placed at imminent risk of additional fraudulent transactions and other concrete, tangible harm.

11. Defendant Deloitte Consulting LLP is a Delaware corporation with its principal place of business in New York, New York.

III. JURISDICTION AND VENUE

12. This Court has subject matter jurisdiction over this case pursuant to 28 U.S.C. § 1332(d), the Class Action Fairness Act, which affords federal courts with original jurisdiction over cases where any member of the plaintiff class is a citizen of a state different from any defendant, and where the amount in controversy exceeds $5,000,000, exclusive of interest and costs. Plaintiff, being a resident of the State of Illinois, is diverse from Defendant, which is headquartered in New York and incorporated in Delaware. Plaintiff alleges that, in the aggregate, the claims of all Class members exceed $5,000,000, exclusive of interest and costs.

13. This Court has personal jurisdiction over Defendant because Defendant maintains its headquarters in this District.

---

[1] See, https://www.cnbc.com/2020/02/24/how-to-improve-your-credit-score-right-away.html (Last viewed: June 8, 2020).

14. This Court is the proper venue for this case pursuant to 28 U.S.C. § 1391(b) because Defendant does business in this District, and is subject to personal jurisdiction here, and because a substantial part of the events giving rise to this action occurred in this District.

IV. FACTUAL BACKGROUND

15. The PUA, established pursuant to the Coronavirus Aid Care and Economic Security, or "CARES" Act, expanded unemployment insurance eligibility to self-employed workers, freelancers, independent contractors, and part-time contractors impacted by the COVID-19 pandemic.

16. Because the PUA program required a new processing system to handle these different types of claims, which are distinct from regular unemployment claims, states including Ohio, Illinois, and Colorado contracted with Deloitte to design a cloud-based portal system.

17. Deloitte launched the system on or about May 11, 2020, knowing at that time that safeguarding unemployment applicants' PII is of critical importance due to the serious harm flowing from a compromise of that data, particularly when it involves private financial information like an applicant's social security number. The U.S. Federal Trade Commission ("FTC") in fact publishes a guide for businesses regarding the proper protection of PII. *See Protecting PII: A Guide for Business* (October 2016)[2].

18. On May 15, 2020, Illinois State Representative Terri Bryant sent a letter to Illinois Governor Pritzker informing him that a constituent of hers had accessed a spreadsheet on the IDES

[2] Available at https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business.

portal that contained the PII for thousands of unemployment applicants, including name, address, social security number, and unemployment claimant ID number.[3]

19. Deloitte's system had allowed applicants' PII to be exposed to the public, including applicants' social security number, bank account and routing numbers, and other sensitive information.[4]

20. CDLE was next, confirming on May 18, 2020 that Deloitte's system had allowed third-party access to applicant's PII.

21. On May 20, 2020, ODJFS sent applicants an email notifying them that Deloitte's system had exposed Ohio applicants' PII to the public.

22. Plaintiff became aware that her information had been exposed through the PUA system when Plaintiff received a communication regarding the breach on May 21, 2020 as described above.

23. Defendant was aware of its duty to safeguard the PII that it collected, and unemployment applicants relied on Defendant to take every precaution to safeguard their PII.

24. Plaintiff provided PII to Defendant when Plaintiff applied for unemployment benefits through the web portal it designed, built and maintained.

25. Defendant failed to safeguard Plaintiff's PII and, as a result, Plaintiff's PII was exposed as part of the Data Breach.

---

[3] https://repbryant.com/2020/05/16/rep-bryant-demands-governor-answer-questions-involving-potential-massive-ides-unemployment-applicant-data-breach/.

[4] https://www.fox13memphis.com/news/local/hackers-leak-over-20000-unemployment-applicants-bank-information/OL2CZV7GM5DLLPPI3QTPCHDRNM/

26. As a result of the Data Breach, Plaintiff has expended time and suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the future consequences of the Data Breach including investigating the information compromised and how best to ensure Plaintiff is protected from potential identity theft and fraud, which efforts are continuous and ongoing.

27. Plaintiff has also suffered injury directly and proximately caused by the Data Breach including: (a) theft of her valuable PII; (b) the imminent and certain impeding injury flowing from fraud and identity theft posed by their PII being placed in the hands of hackers; (c) loss of the benefit of the bargain with Defendant to provide adequate and reasonable data security – i.e., the difference in value between what Plaintiff should have received from Defendant when Defendant represented Plaintiff's PII would be protected by reasonable data security, and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security and failing to protect Plaintiff's PII; and (d) continued risk to Plaintiff's PII, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate an adequate measures to protect the PII that was entrusted to it.

28. Defendant's failure to safeguard Plaintiff's and the Class's PII is particularly dangerous here where the exposed sensitive information includes social security numbers. According to Paige Schaffer, CEO of Generali Global Assistance's identity and digital protection

services global unit, "where social security numbers are involved, victims' identity fraud risk remains elevated, if not for several years then for life."[5]

29. Defendant itself acknowledged the imminent harm caused by the Data Breach, as it is offering 12 months of free credit monitoring to all PUA unemployment applicants in the affected states.

V. CLASS ACTION ALLEGATIONS

30. Plaintiff brings this action individually and as a class action on behalf of the following nationwide and Illinois Subclasses (collectively, the "Class"):

Nationwide Class

All persons in the United States (including its Territories and the District of Columbia) whose PII was compromised as a result of the Data Breach.

Illinois Subclass

All persons in Illinois whose PII was compromised as a result of the Data Breach.

31. Excluded from the Class are Deloitte Consulting LLP and its officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Class are any judicial officer presiding over this matter, members of their immediate family, and members of their judicial staff.

32. The members of the Class are so numerous and geographically dispersed that joinder would be impracticable. Although the precise number of individuals in the Class is unknown at this time, upon information and belief the number is in the hundreds of thousands at

[5] https://www.insurancebusinessmag.com/us/news/cyber/consumers-data-exposed-for-years-following-breach-incidents-178390.aspx.

least. Class members are readily identifiable from information and records in Defendant's possession, custody, or control

33. There is a well-defined community of interest in the common questions of law and fact affecting the Class members. These common legal and factual questions include, but are not limited to:

a. whether Defendant owed a duty to use reasonable care to avoid causing foreseeable risk of harm to Plaintiff and members of the Class when obtaining, storing, using, and managing PII, including taking action to safeguard such data;

b. whether Defendant failed to safeguard Plaintiff's and the Class members' PII;

c. whether Defendant implemented and maintained data security measures that it knew or should have known were unreasonable and inadequate to protect PII;

d. whether Defendant negligently allowed PII to be accessed, used, or disclosed by third parties;

e. whether Defendant failed to timely and adequately notify Plaintiff and members of the Class that its data systems were breached;

f. whether Plaintiff and members of the Class were injured;

g. whether Defendant's actions and inactions failed to provide reasonable security proximately caused the injuries suffered by Plaintiff and members of the Class;

h. whether Plaintiff and members of the Class are entitled to damages and, if so, the measure of such damages; and

i. whether Plaintiff and members of the Class are entitled to injunctive, equitable, declaratory and/or other relief, and if so, the nature of such relief.

34. Plaintiff's claims are typical of the claims of the absent class members and have a common origin and basis. Plaintiff and absent Class members are all injured by the Data Breach. Plaintiff's claims arise from the same practices and course of conduct giving rise to the claims of the absent Class members and are based on the same legal theories. If prosecuted individually, the claims of each Class member would necessarily rely upon the same material facts and legal theories and seek the same relief. Plaintiff's claims arise from the same practices and course of conduct that give rise to the other Class members' claims and are based on the same legal theories.

35. Plaintiff will fully and adequately assert and protect the interests of the absent Class members and have retained Class counsel who are experienced and qualified in prosecuting class action cases similar to this one. Neither Plaintiff nor Plaintiff's attorneys have any interests contrary to or conflicting with the interests of absent Class members.

36. The questions of law and fact common to all Class members predominate over any questions affecting only individual class members.

37. A class action is superior to all other available methods for the fair and efficient adjudication of this lawsuit because individual litigation of the absent Class members' claims is economically infeasible and procedurally impracticable. Class members share the same factual and legal issues and litigating the claims together will prevent varying, inconsistent, or contradictory judgments, and will prevent delay and expense to all parties and the court system through litigating multiple trials on the same legal and factual issues. Class treatment will also permit Class members to litigate their claims where it would otherwise be too expensive or inefficient to do so. Plaintiff knows of no difficulties in managing this action that would preclude its maintenance as a class action.

38. Additionally, the prosecution of separate actions by individual Class members would create a risk of inconsistent or varying adjudications with respect to individual Class members that would establish incompatible standards of conduct for Defendant. Such individual actions would create a risk of adjudications that would be dispositive of the interests of other Class members and impair their interests. Defendant, through its uniform conduct, acted or refused to act on grounds generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the Class as a whole.

VI. CAUSES OF ACTION

COUNT I – NEGLIGENCE
(On Behalf of Plaintiff and the Classes)

39. Plaintiff repeats and realleges each and every allegation contained above as if fully set forth herein.

40. Defendant requires Plaintiff and Class members to submit PII in order to obtain unemployment benefits through the PUA system.

41. Defendant knew or should have known the risks inherent in collecting and storing the PII of plaintiff and the Class members.

42. Defendant owed a common law duty to use reasonable care to avoid causing foreseeable risk of harm to Plaintiff and members of the Class when obtaining, storing, using, and managing PII, including taking action to reasonably safeguard such data and providing notification to Plaintiff and the Class members of any breach in a timely manner so that appropriate action can be taken to minimize or avoid losses.

43. Numerous courts and legislatures have recognized the existence of a specific duty to reasonably safeguard PII.

44. Plaintiff and the Class members were the intended beneficiaries of Defendant's duty to safeguard PII, creating a special relationship between them and Defendant. Indeed, Plaintiff and the Class members entrusted Defendant with their PII in order to obtain necessary unemployment benefits in the midst of a pandemic, and they relied on Defendant to maintain reasonable and adequate security measures in order to protect that PII from disclosure. Only Defendant was in a position to ensure that its systems were sufficient to protect the PII that Plaintiff and the Class members entrusted to it.

45. It was foreseeable that injury to Plaintiff and Class members would result from Defendant's active mishandling of PII including, but not limited to, Defendant's failure to use reasonable security measures to protect such PII.

46. Defendant assumed the duty to act with reasonable care in managing its data, and to use reasonable security measures to protect such data, including the duty to comply with data security industry standards.

47. Defendant knew or should have known of the significant risk that its computer systems could be breached, in particular in light of the numerous recent data breach incidents around the country.

48. Defendant breached its common law duties and industry standards of care—and was negligent—by actively mishandling the PII of Plaintiff and Class members and by failing to use reasonable and adequate security measures to protect that PII from the hackers who perpetrated the Data Breach and by failing to identify the Data Breach in a timely manner.

49. Defendant breached its duties by: (a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized disclosure, misuse, alteration, destruction

or other compromise of such information; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; and/or (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein.

50. As a direct and proximate result of Defendant's negligent acts of misfeasance and nonfeasance, Plaintiff and Class members have suffered and continue to suffer injury, including loss of time and productivity through efforts to ameliorate, mitigate, and deal with the future consequences of the Data Breach; theft of their valuable PII; and the imminent and certain impeding injury flowing from fraud and identity theft posed by their PII being placed in the hands of unauthorized third parties.

COUNT II – NEGLIGENCE PER SE
(On Behalf of Plaintiff and the Classes)

51. Plaintiff repeats and realleges each and every allegation contained above as if fully set forth herein.

52. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair practice of failing to act reasonably in the management of the data, and to use reasonable security measures to protect such data by companies such as Defendant. FTC guidelines, publications, and consent orders described above also form the basis of Defendant's duty.

53. Defendant violated Section 5 of the FTC Act (and similar state statutes) by mishandling Plaintiff's and the Class members' PII, failing to use reasonable measures to protect the PII, and by not complying with applicable industry standards.

54. Defendant's violation of Section 5 of the FTC Act (and similar state statutes) constitutes negligence per se.

55. Plaintiff and the Class are within the scope of persons that Section 5 of the FTC Act (and similar state statutes) was intended to protect.

56. Furthermore, the harm that has occurred is the type of harm the FTC Act (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and the Class here.

57. As a direct and proximate result of Defendant's negligence per se, Plaintiff and the Class have suffered and continue to suffer injury and damages, including loss of time and productivity through efforts to ameliorate, mitigate, and deal with the future consequences of the Data Breach; theft of their valuable PII; and the imminent and certain impeding injury flowing from fraud and identity theft posed by their PII being placed in the hands of unauthorized third parties.

COUNT III – BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Classes)

58. Plaintiff repeats and realleges each and every allegation contained above as if fully set forth herein.

59. Defendant invited and induced unemployment applicants, including Plaintiff and Class members, to use its PUA portal.

60. Implicit in Defendant's offer was that it would safeguard the PII using reasonable or industry-standard means.

61. Based on this understanding, Plaintiff and Class members accepted Defendant's offer and provided their PII to Defendant.

62. Plaintiff and class members would not have provided their PII had they known Defendant would not safeguard it as impliedly promised.

63. Plaintiff and class members fully performed their obligations under the implied contracts with Defendant.

64. Defendant breached the implied contracts by failing to safeguard Plaintiffs' and class members' PII, causing direct and substantial damages to Plaintiff and class members.

COUNT IV – BAILMENT
(On Behalf of Plaintiff and the Classes)

65. Plaintiff repeats and realleges each and every allegation contained above as if fully set forth herein.

66. Plaintiff and Class members provided, or authorized disclosure of, their PI to Defendant for the exclusive purpose of applying for unemployment benefits and using the associated portal.

67. In allowing their PI to be made available to Defendant, Plaintiff and Class members intended and understood that Defendant would adequately safeguard their PII.

68. For its own benefit, Defendant accepted possession of Plaintiff's and Class members' PII for purpose of making available its own service.

69. Defendant understood that Plaintiff and Class members expected Defendant to adequately safeguard their personal information. Accordingly, a bailment was established for the parties' mutual benefit.

70. During the bailment, Defendant owed a duty to Plaintiff and the Class members to exercise reasonable care, diligence, and prudence in protect their PII.

71. Defendant breached its duty of care by failing to take appropriate measures to safeguard Plaintiff's and the Class members' PII, resulting in the unauthorized disclosure of their PII.

72. As a direct and proximate result of Defendant's breach of its duty, Plaintiff and Class members suffered damages that were reasonably foreseeable to Defendant.

73. As a direct and proximate result, the PII Plaintiff and the Class members entrusted to Defendant during the bailment was damaged, and its value diminished.

COUNT V – UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Classes)

74. Plaintiff repeats and realleges each and every allegation contained above as if fully set forth herein.

75. Defendant, by way of its acts and omissions, knowingly and deliberately enriched itself by saving the costs it reasonably should have expended on security measures to secure Plaintiff's and Class members' PII.

76. Instead of providing for a reasonable level of security that would have prevented the breach—as is common practice among companies entrusted with such PII—Defendant instead consciously and opportunistically calculated to increase its own profits at the expense of Plaintiff and Class members.

77. Nevertheless, Defendant continued to obtain the benefits conferred on them by Plaintiffs and Class Members.

78. Plaintiff and Class members suffered harm as a direct and proximate result, in the forms of, *inter alia*, attempted identity theft, time and expenses mitigating harms, diminished value of PII, loss of privacy, and increased risk of harm.

79. Defendant profited from its acts and omissions.

80. Based on these acts and omissions, which caused the unauthorized public release of Plaintiff's and the Class members' sensitive PII, it would be inequitable, unconscionable, and unlawful to permit Defendant to retain the benefits it derived as a consequence of its conduct.

COUNT VI – VIOLATION OF NEW YORK GENERAL BUSINESS LAW § 349
(On Behalf of Plaintiff and the Classes)

81. Plaintiff repeats and realleges each and every allegation contained above as if fully set forth herein.

82. New York's General Business Law, Section 349, prohibits "[d]eceptive acts and practices in the conduct of any business, trade or commerce or in the furnishing of any service in this state." Violations of Section 349 are unlawful an actionable by aggrieved consumers.

83. At all times herein, Defendant was subject to the requirements of Section 349, which it breached in connection with the data breach associated with the PUA program intended to provide services in the furnishing of unemployment benefits to the public at large.

84. Defendant violated Section 349 by disclosing Plaintiff's and Class Members' PII as a result of the Data Breach.

85. Because of the Data Breach, Plaintiff and Class Members suffered damages that were attributable to Defendant's failure to maintain the confidentiality in their PI.

86. Pursuant to Section 349(h), Plaintiff and Class Members are entitled to actual damages, statutory damages, injunctive relief, attorneys' fees and costs.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all others similarly situated, respectfully requests judgment against Defendant as follows:

i. For an order certifying this action as a class action, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding Plaintiff to be a proper representative of the Class and Subclass.

ii. For a permanent injunction and any other equitable relief as necessary to protect the interest of the Class, including:

1. An order declaring Defendant's conduct alleged herein unlawful and prohibiting Defendant from engaging in the wrongful and unlawful acts.

2. Requiring Defendant to develop a security protocol to include standards to:

a. protect all data collected or received through the course of its business in accordance with the FTC Act and other federal, state, and local laws, and best practices under industry standards;

b. design, maintain, and test its computer systems to ensure that PII in its possession is adequately secured and protected;

c. engage third-party security auditors and internal security personnel to conduct testing, including simulated attacks, penetration testing, and audits on Defendant's systems on a periodic basis and ordering it to promptly correct any problems or issues detected by those auditors;

d. audit, test, and train their security personnel to run automated security monitoring, aggregation, filtering and reporting on log information in a unified manner;

e. encrypt all PII;

f. purge, delete, and destroy in a reasonably secure and timely manner any PII no longer necessary for their provision of goods and services;

g. routinely and continually conduct internal training and education to inform personnel how to identify and contain a breach and what to do in response;

h. deploy appropriate and up-to-date SPAM filters, web filters, and antivirus solutions;

i. employ standards for password expiration and complexity; and

j. educate its employees and conduct training sessions with mock phishing exercises.

3. Requiring Defendant to disclose any future data breaches in a timely and accurate manner.

iii. An award of compensatory damages, restitution, statutory damages, punitive damages, and/or attorneys' fees and costs recoverable under the claims pleaded herein, as well as any such other relief as is just and proper.

VIII. DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury on all issues so triable

Date: June 8, 2020

Respectfully submitted,

/s/ Kyle A. Shamberg
Katrina Carroll*
Kyle A. Shamberg
CARLSON LYNCH LLP
111 W. Washington Street, Suite 1240
Chicago, Illinois 60602
Telephone: (312) 750-1265
Facsimile: (412) 231-0246
Email: kcarroll@carlsonlynch.com
kshamberg@carlsonlynch.com

Jonathan M. Jagher*
Kimberly A. Justice*
FREED KANNER LONDON & MILLEN LLC
923 Fayette Street
Conshohocken, PA 19428
P. (610) 234-6487
jjagher@fklmlaw.com
kjustice@fklmlaw.com

Attorneys for Plaintiff and the Proposed Classes

*to be admitted *pro hac vice*